Alternative Chains, Valute, <phrase role="keep-together">e Applicazioni</phrase>

Bitcoin è stato il risultato di 20 anni di ricerca in sistemi distribuiti e valute, e ha portato a una tecnologia rivoluzionaria nel suo campo: il meccanismo di consenso decentralizzato basato sulla proof of work. Questa invenzione al cuore di bitcoin ha generato un'onda di innovazione in valute, servizi finanziari, economia, sistemi distribuiti, sistemi di votazione, corporate governance e contratti.

In questo capitolo esamineremo le molte ramificazioni del Bitcoin e le invenzioni blockchain: le catene alternative, le valute e le applicazioni costruite dopo l'introduzione di questa tecnologia nel 2009. Per lo più, vedremo monete alternative, o *alt coins*, che sono valute digitali implementate utilizzando lo stesso modello di progettazione del bitcoin, ma con una blockchain e rete completamente diverse.

Per ogni alt-coin menzionato in questo capitolo, 50 o più non saranno nemmeno menzionati, scatenando urla di rabbia dai creatori e addirittura dai suoi stessi fan. Lo scopo di questo capitolo è quello di non valutare o giudicare alt-coin, e non è neppure quello di menzionare i progetti più famosi basandosi su di qualche fatto soggettivo. Invece, evidenzieremo alcuni esempi per mostrare la varietà e ampiezza di progetti possibili da aggiungere all'ecosistema, notando le ultime innovazioni precedentemente irrealizzabili o con particolarità significative. Alcuni dei più interessanti esempi di alt-coin sono in fatti fallimenti completi da una prospettiva monetaria. Questo forse le rende anche molto interessanti da studiare e evidenziando il fatto che questo capitolo non dovrebbe essere usato come una guida di investimento (in criptovaluta).

Con nuove monete introdotte ogni giorno, sarebbe impossibile non perdere qualche moneta importante, forse proprio quella che cambierà la storia. Il tasso di innovazione è ciò che rende questo momento così eccitante e garantisce che questo capitolo sarà incompleto ed obsoleto non appena pubblicato.

Una Tassonomia di Valute Alternative e Chains

Bitcoin e' un progetto open source, ed il suo codice e' stato usato come base per molti altri progetti software. La piu comune forma di software prodotta dal codice sorgente di bitcoin sono le monete decentralizzate alternative, o *alt coin*, che usano gli stessi elementi costitutivi di base delle monete digitali.

Ci sono una serie di strati (layer) di protocolli implementati sopra la blockchain di bitcoin. Queste *meta coin*, *meta chain*, o *blockchain apps* utilizzano la blockchain come una piattaforma applicativa o estendono il protocollo bitcoin aggiungendo alcuni protocolli su di un layer addizionale. Esempi di questo includono i Colored Coin, Mastercoin, NXT e Counterparty.

Nella successiva sezione, esamineremo alcune alt coin degne di nota, come Litecoin, Dogecoin, Freicoin, Primecoin, Peercoin, Darkcoin, e Zerocoin. Queste alt coin sono note per ragioni storiche o perche sono buoni esempi di uno specifico tipo di innovativa alt coin, non perche sono le piu

redditizie o "le migliori" alt coin.

Oltre alle alt coin, vi sono anche un numero di implementazioni di blockchain alternative che non sono realmente "monete," che chiamo *alt chain*. Queste alt chain implementano un algoritmo di consenso distribuito e un registro distribuito come piattaforma per contratti, registrazioni di titoli o altre applicazioni. Le alt chain utilizzano gli stessi "mattoni" e talvolta utilizzano anche una moneta o un token come metodo di pagamento, ma il loro primo scopo non è quello di realizzare un sistema monetario. Osserveremo Namecoin e Ethereum come esempi di alt chain.

Infine, ci sono un numero di bitcoin competitor che offrono valuta digitale o reti di pagamento digitali, ma senza l'impiego di un registro decentralizzato o un meccanismo di consenso basato su proof of work, come Ripple ed altri. Queste tecnologie non-blockchain sono al di fuori dell'intento di questo libro e non verranno coperte in questo capitolo.

Piattaforme di Meta Coin

Meta coin e meta chain sono dei livelli di software implementati su bitcoin, sia adottando una moneta dentro una moneta, o una piattaforma/protocollo di substrato all'interno del sistema bitcoin. Questi livelli di funzioni estendono il nucleo del protocollo di bitcoin ed aggiungono specifiche e funzionalità attraverso la codifica di ulteriori dati all'interno delle transazioni di bitcoin ed indirizzi bitcoin. Le prime implementazioni di meta-monete usarono diversi accorgimenti per aggiungere metadati alla blockchain di bitcoin, usando ad esempio gli indirizzi bitcoin per codificare dati o utilizzando i campi di transazioni inutilizzati (come il campo della sequenza di transazioni) per codificare metadati riguardo il livello di protocollo aggiunto. Fin dall'introduzione dell'opcode script di transazione OP_RETURN, le meta monete sono state in grado di registrare metadati piu direttamente nella blockchain, e molte stanno migrando per usarlo.

Colored Coin

Colored coins e' un meta protocollo che copre informazioni riguardo un piccolo ammontare di bitcoin. Una moneta "colorata" e' una quantita di bitcoin riadattato per esprimere un altro asset. Immagina, ad esempio, di prendere un banconota da 1 dollaro e di apporci un timbro che dice, "Questo e' un certificato azionario dell'azienda Acme" Ora il dollaro serve due obiettivi: e' una banconota ed anche un certificato azionario. Siccome e' piu redditizia come azione, non vorresti usarla per comprare caramelle, quindi effettivamente non e' piu utile come valuta. Le Colored coin funziano nella stesso modo, convertendo una specifica, alquanto piccola, somma di bitcoin in un certificato di scambio che rappresenta un altro asset. Il termine "colore" richiama all'idea di conferire un significato speciale attraverso l'aggiunta di un attributo come un colore-- e' una metafora, non una reale associazione di colore. Non ci sono colori in colored coin.

Le monete Colorate sono gestite da specifici wallet che registrano ed interpretano i metadati allegati alle bitcoin colorate. Usando tale wallet, l'utente convertira l'ammontare di bitcoin da monete incolori in monete colorate attraverso l'aggiunta di una etichetta che ha un significato particolare. Ad esempio, un'etichetta potrebbe rappresentare certificati azionari, coupons, proprieta' reale, materie prime, o token collezionabili. E' interamente a discrezione degli utenti di monete colorate di assegnare ed interpretare il signifcato di "colore" associato ad una specifica moneta. Per colorare le monete, l'utente definisce i metadati associati, come il tipo di emissione, se puo essere suddiviso in unita piu piccole, un simbolo e descrizione, ed altre informazioni correlate.

Una volta colorate, queste monete possono essere acquistate e vendute, suddivise, ed aggregate, e ricevere il pagamento di dividendi. Le monete colorate possono inoltre essere "incolore" rimuovendo la particolare associazione e riscattate per il loro valore nominale in bitcoin.

Per dimostrare l'uso di monete colorate, abbiamo creato un gruppo di 20 monete colorate con simbolo "MasterBTC" che rappresenta coupons per una copia gratuita di questo libro in Il profilo dei meta-dati di colored coin registrati come coupon per una copia gratuita del libro. Ciascuna unita di MasterBTC, rappresentata da queste monete colorate, possono ora essere vendute o cedute a qualsiasi utente bitcoin con un wallet compatibile con le monete colorate, che possono essere trasferite successivamente ad altri o riscattate con l'emittente in cambio di una copia gratuita del libro. Questo esempio di monete colorate puo essere visto qui.

Example 1. Il profilo dei meta-dati di colored coin registrati come coupon per una copia gratuita del libro

```
{
  "source_addresses": [
    "3NpZmvSPLmN2cVFw1pY7gxEAVPCVfnWfVD"
  ],
  "contract_url":
"https://www.coinprism.info/asset/3NpZmvSPLmN2cVFw1pY7gxEAVPCVfnWfVD",
  "name_short": "MasterBTC",
  "name": "Free copy of \"Mastering Bitcoin\"",
  "issuer": "Andreas M. Antonopoulos",
  "description": "This token is redeemable for a free copy of the book \"Mastering
Bitcoin\"",
  "description_mime": "text/x-markdown; charset=UTF-8",
  "type": "Other",
  "divisibility": 0,
  "link_to_website": false,
  "icon_url": null,
  "image_url": null,
  "version": "1.0"
}
```

Mastercoin

Mastercoin e' un protocollo di livello in cima a bitcoin che supporta una piattaforma per diverse applicazioni ampliando il sistema bitcoin. Mastercoin usa la valuta MST come token per effettuare transaziondi di Mastercoin anche se non e' principalmente una moneta. Piuttosto, e' una piattaforma per la costruzione di altre cose, come monete utente, token di smart property, borse di scambio di asset decentralizzate, e contratti. Pensare a Mastercoin come ad un protocollo di livello applicativo in cima al livello di trasporto delle transazioni finanziarie, nello stesso modo in cui HTTP gira in cima a TCP.

Mastercoin opera principalmente attraverso transazioni inviate da e verso uno speciale indirizzo bitcoin chiamato l'indirizzo "exodus" (1EXoDusjGwvnjZUyKkxZ4UHEf77z6A5S4P), proprio come HTTP utilizza una specifica porta TCP (porta 80) per distinguere il suo traffico dal resto del traffico TCP. Il protocollo Mastercoin sta transitando gradualmente dall'usare lo specifico exodus address e

firme multiple ad usare l'operatore bitcoin OP_RETURN per codificare metadati di transazioni.

Counterparty

Counterparty e' un altro protocollo di livello implementato in cima a bitcoin. Counterparty abilita le monete utente, token negoziabili, strumenti finanziari, borse di scambio di asset decentralizzate, ed altre caratteristiche. Counterparty e' implementato principalmente usando l'operatore OP_RETURN nel linguaggio di scripting di bitcoin per registrare metadati che arricchiscono le transazioni di bitcoin di significato aggiuntivo. Counterparty usa la moneta XCP come token per gestire le transazioni.

Gli Alt Coin

La vasta maggioranza delle alt coin sono derivati del codice sorgente di bitcoin, anche noti come "fork". Alcuni sono implementati "da zero" basati sul modello blockchain ma senza usare il codice sorgente di bitcoin. Alt coin ed alt chain (nella prossima sezione) sono entrambi separate implementazioni della tencologia blockchain ed entrambe le forme adottano la propria blockchain. La differenza nei termini sta per indicare che alt coin sono principalmente utilizzate come valuta, mentre le alt chain sono usate per altri scopi, non principalmente come valute.

In senso stretto, il primo grande fork "alt" del codice di bitcoin non era un'altcoin ma la alt chain *Namecoin*, di cui parleremo nella prossima sezione.

Basato sulla data dell'annuncio, la prima alt coin ad essere un fork di bitcoin apparve nell'agosto del 2011; era chiamata *IXCoin*. IXCoin modifico alcuni parametri di bitcoin, accellerando specificatamente la creazione di moneta attraverso l'incremento del compenso a 96 monete per blocco.

Nel settembre del 2011, *Tenebrix* venne lanciato. Tenebrix era la prima cryptovaluta ad implementare un alternativo algoritmo proof-of-work, cioe'*script*, un algoritmo originalmente progettato per il password streching (brute-force resistance). L'obiettivo dichiarato di Tenebrix era quello di realizzare una moneta che fosse resistente al mining con GPUs e ASICs, utilizzando un algoritmo ad alto dispendio di memoria. Tenebrix non ebbe successo come moneta, ma fu la base per Litecoin, che ha goduto di grande successo ed ha prodotto centinaia di cloni.

Litecoin, oltre ad usare script come algoritmo di proof-of-work, implementa anche un tempo di generazione-blocco piu rapido, fissato a 2.5 minuti rispetto ai 10 minuti di bitcoin. La valuta risultante e' proposta come "argento rispetto all'oro di bitcoin" ed e' intesa come una valuta leggera alternativa. A causa del tempo di conferma piu rapido e del limite di 84 milioni di moneta totale, molti sostenitori di Litecoin pensano sia più adatta per transazioni commerciali rispetto a bitcoin.

Alt coin continuarono a proliferare nel 2011 e 2012, sia basate su bitcoin, sia su Litecoin. Nel 2013, c'erano 20 alt coin in lizza per una posizione sul mercato. Al termine del 2013, questo numero esplose a 200, con un 2013 che divenne rapidamente "L'anno delle alt coin". La crescita di alt coin continuo nel 2014, con piu di 500 alt coin esistenti al momento della stesura. Oggi, piu della meta delle alt coin, sono cloni di Litecoin.

Creare un alt coin e' semplice, che e' il motivo per cui ce ne sono più 500. Molte di loro, differiscono molto leggermente da bitcoin e non offrono nulla degno di studio. Moltre sono, infatti, solo tentativi

di arricchire i loro creatori. Tra le imitazioni e schemi di pump-and-dump, ci sono, tuttavia, alcune eccezioni degne di nota ed innovazioni molto importanti. Queste alt coin adottano approcci radicalmente diversi o aggiungono una significativa innovazione al modello del design di bitcoin. Ci sono tre principali aree dove queste alt coin si diversificano da bitcoin:

- Politica monetaria differente
- Differenti meccanismi di consenso o proof of work
- Caratteristiche specifiche, come una forte anonimità

Per ulteriori informazioni, consulta questo http://mapofcoins.com [linea temporale grafica di tutti gli alt coin e delle alt chain].

Valutare un Alt Coin

Con cosi tante alt coin in circolazione, come si puo decidere queli sono degne di nota? Alcune alt coin tentano di raggiungere un'ampia distribuzione ed uso come monete. Altre sono laboratori per sperimentare diverse caratteristiche e modelli monetari. Molte sono solamente uno schema per arricchirsi velocemente dai loro creatori. Per valutare le alt coin, io guardo alla loro definizione delle caratteristiche ed alle metriche di mercato.

Ecco un po di domande da farsi riguardo come un altcoin si differenzia da bitcoin:

- L'alt coin introduce una innovazione significativa?
- C'è una differenza sufficientemente coinvolgente per attrarre altri utenti fuori da bitcoin?
- L'alt coin si rivolge ad un interessato mercato di nicchia o specifica applicazione?
- Puo l'alt coin attrarre abbastanza miner per essere protetto da attacchi riguardo al consenso delle transazioni?

Ecco un po delle metriche finanziare e di mercato chiave da considerare:

- Qual'è la capitalizzazione totale di mercato di un'alt coin?
- Qual'è la stima del numero di utenti/wallet che ha l'alt coin?
- Quanti commercianti accettano l'alt coin?
- Quante transazioni giornaliere (volume) sono eseguite sull'alt coin?
- Quanto valore (fiat) è transato ogni giorno?

In questo capitolo, ci concentreremo principalmente sulle caratteristiche tecniche e sul potenziale d'innovazione degli alt coin rappresentati dal pimo gruppo di domande.

Parametri Monetari Alternativi: Litecoin, Dogecoin, Freicoin

Bitcoin ha pochi parametri monetari che le conferiscono caratteristiche distintive di una moneta deflazionaria a emissione fissa. E' limitata a 21 milioni di unita' di moneta principali (o 21 10^24 unita minori), e ha un tasso di emissione geometricamente decrescente, ed ha un "battito" di 10 minuti a blocco, che controlla la velocità della conferma di una transazione e la generazione di moneta. Molte alt coin hanno truccato i parametri principali per raggiungere diverse politiche

monetarie. Tra le centinaia di alt coin, alcune dei più noti esempi includono i seguenti.

Litecoin

Uno dei primi altcoin, rilasciato nel 2011. Litecoin é la seconda valuta digitale con più successo dopo Bitcoin. Le sue innovazioni principali furono l'uso di *scrypt* come algoritmo di proof-of-work (ereditato da Tenebrix) e i suoi parametri della moneta più veloci/leggeri.

- Tempo di generazione blocco: 2.5 minuti
- Moneta totale: 84 milioni di unità nel 2140
- Algoritmo di consenso: proof of work Scrypt
- Capitalizzazione di mercato: $160 milioni a meta del 2014

Dogecoin

Dogecoin fu rilasciata nel dicembre del 2013, basata su un fork di Litecoin. Dogecoin e' nota perche ha una politica monetaria di rapida emissione ed un cap monetario molto alto, per incoraggiare la spesa e le mance. Dogecoin e anche nota perche inizio per gioco ma divenne alquanto popolare, con un'ampia ed attiva communita, prima di calare rapidamente nel 2014.

- Tempo di generaizione blocco: 60 secondi
- Moneta totale: 100,000,000,000 (100 miliardi) di Doge nel 2015
- Algoritmo di consenso: proof of work Scrypt
- Capitalizzazione di mercato: $12 milioni a metà del 2014

Freicoin

Freicoin venne introdotta nel luglio del 2012. Si tratta di una *deurrage currency*, cioe' con un tasso di interesse negativo per il valore memorizzato. Il valore memorizzato in Freicoin e' fissato ad una commissione APR di 4.5%, per incoraggiare il consumo e scoraggiare l'ammassamento di denaro. Freicoin e' degno di nota in quanto implementa una politica monetaria che e' l'esatto opposto della politica deflazionistica di Bitcoin. Freicoin non ha visto alcun successo come moneta, ma e' un interessante esempio della varietà delle politiche monetarie che possono essere espresse dalle alt coin.

- Tempo di generazione blocco: 10 minuti
- Moneta totale: 100 millioni di unità nel 2140
- Algoritmo di consenso: proof of work SHA256
- Capitalizzazione di mercato: $130,000 a metà del 2014

Innovazioni sul consenso: Peercoin, Myriad, Blackcoin, Vericoin, NXT

Il meccanismo di consenso di Bitcoin e' basato sulla proof of work usando l'algoritmo SHA256. La prima alt coin introdusse scrypt come algoritmo di proof-of-work alternativo, come un modo di minare piu CPU-friendly e meno sucettibile di centralizzazione con ASICs. Da allora, l'innovazione nel meccanismo di consenso ha continuato a passo frenetico. Diverse alt coin adottarono una

varieta di algoritmi simili a scrypt, scrypt-N, Skein, Groestl, SHA3, X11, Blake, ed altri. Alcune alt coin combinarono piu algoritmi come proof of work. Nel 2013, vedemmo l'invenzione di un'alternativa alla proof of work, chiamata *proof of stake*, che forma la base di molte alt coin moderne.

Proof of stake e' un sistema per cui proprietari esistenti di una moneta possono "conservare" moneta come collaterale fruttifero. Con qualcosa di simile ad un certificato di deposito (CD), i partecipanti possono riservare una porzione della loro riserva di valuta, mentre guadagnano un rendimento sugli investimenti nella creazione di nuova moneta (emessa come pagamenti di interessi) e commissioni di transazione.

Peercoin

Peercoin è stato introdotto nell'Agosto 2012 ed e' la prima alt coin ad usare un'algoritmo di proof-of-work e proof-of stake ibrido per emettere nuova valuta.

- Tempo di generazione blocco: 10 minuti
- Moneta totale: Nessun limite
- Algoritmo di consenso: (Ibrido) proof-of-stake con proof-of-work iniziale
- Capitalizzazione di mercato: $14 millioni a metà del 2014

Myriad

Myriad venne introdotta nel Febbraio del 2014 ed e' nota perche usa 5 diversi algoritmi proof-of-work (SHA256d, Scrypt, Qubit, Skein, o Myriad-Groestl) simultaneamente, la cui difficoltà varia per ogni algoritmo sulla base della partecipazione di minatori. L'intento e' di rendere Myriad immune dalla specializzazione e centralizzazione degli ASIC tanto quanto piu resistente ad attacchi di consenso, in quanto piu algoritmi di mining dovrebbero essere attaccati contemporaneamente.

- Generazione blocco: 30 secondi di media (target di 2.5 minuti per ogni algoritmo di mining)
- Moneta totale: 2 miliardi nel 2024
- Algoritmo di consenso: Proof-of-work multi-algoritmo
- Capitalizzazione di mercato: $120,000 a metà del 2014

Blackcoin

Blackcoin venne introdotta nel Febbraio del 2014 ed usa un algoritmo di consenso proof-of-stake. E' anche nota per aver introdotto "multipools", un tipo di mining pool che può passare tra diverse alt coin automaticamente, in base alla redditivita'.

- Generazione blocco: 1 minuto
- Moneta totale: Nessun limite
- Algoritmo di consenso: Proof-of-stake
- Capitalizzazione di mercato: $3.7 millioni a metà del 2014

VeriCoin

VeiCoin venne lanciata nel Maggio del 2014. Usa un algoritmo di consenso proof-of-stake con un tasso d'interesse variabile che si regola dinamicamente sulla base delle forze di mercato relative a domanda ed offerta. E', inoltre, la prima alt coin con auto-exchange a bitcoin per pagamenti in bitcoin dal wallet.

- Generazione blocco: 1 minuto
- Moneta totale: Nessun limite
- Algoritmo di consenso: Proof-of-stake
- Capitalizzazione di mercato: $1.1 millioni a metà del 2014

NXT

NXT (pronunciata "Next") e' una "pura" proof-of-stake alt coin, in quanto non fa uso di mining con proof-of-work. NXT e' un'implementazione da zero di una cryptovaluta, non un fork di bitcoin o un'altra alt coin. NXT implementa molte caratteristiche avanzate, incluso un registro di nomi (simile a Namecoin), una borsa di scambio di asset decentralizzata (simile a Colored Coins), sistema sicuro di messaggistica integrato e decentralizzato (simile aBitmessage), e delegazione dello stake (per delegare proof-of-stake ad altri). I sostenitori di NXT la chiamno la cryptovaluta 2.0 o di "prossima generazione".

- Generazione blocco: 1 minuto
- Moneta totale: Nessun limite
- Algoritmo di consenso: Proof-of-stake
- Capitalizzazione di mercato: $30 millioni a metà del 2014

Innovazione Mining ad Obbiettivo-Doppio: Primecoin, Curecoin, Gridcoin

L'algorimto proof-of-work di Bitcoin ha solo uno scopo: proteggere la rete bitcoin. Rispetto alla sicurezza del tradizionale sistema di pagamento, il costo per il mining non e' molto alto. Tuttavia, e' stato criticato da molti come essere "uno spreco". La prossima generazione di alt coin tenta di rivolgersi a questa preoccupazione. Gli algoritmi a duplice scopo proof-of-work risolvono un problema specifico "utile", mentre producono proof of work per proteggere la rete. Il rischio di aggiungere un uso esterno alla sicurezza della moneta è che aggiunge anche un'influenza esterna alla curva offerta / domanda..

Primecoin

Primecoin venne annunciata nel Luglio del 2013. Il suo algoritmo di proof-of-work cerca numeri primi, calcolando Cunningham e le catene prime bi-twin. I numeri primi sono utili in diverse discipline scientifiche. La blockchain di Primecoin contiene i numeri primi scoperti, producendo cosi un registro pubblico di scoperte scientifiche in parallelo al libro di conto pubblico delle transazioni.

- Generazione blocco: 1 minuto
- Moneta totale: Nessun limite

- Algoritmo di consenso: Proof of work con scoperta della catena dei numeri primi
- Capitalizzazione di mercato: $1.3 millioni a metà del 2014

Curecoin

Curecoin venne introdotto nel Maggio del 2013. Combina un algoritmo proof-of-work SHA256 con la ricerca di folding proteico attraverso il profetto Folding@Home. Il folding proteico e' una simulazione computazionalmente intensiva di interazioni biochimiche di proteine, usata per scoprire nuovi bersagli farmacologici per curare le malattie.

- Tempo di generazione blocco: 10 minuti
- Moneta totale: Nessun limite
- Algoritmo di consenso: Proof of work con ricerca sul protein-folding
- Capitalizzazione di mercato: $58,000 a metà del 2014

Gridcoin

Gridcoin venne introdotta nell'Ottobre del 2013. Integra il proof of work basato su scrypt con sussidi di partecipazione in BOINC open grid computing. BOIC—Berkeley Open Infrastructure for Network Computing-- e' un protocollo aperto per la ricerca scientifica nel grid computing, che permette ai partecipanti di condividere i loro cicli di calcolo di riserva per un ampia gamma di calcoli per ricerche accademiche. Gridcoin usa BOINC come piattaforma di calcolo general-purpose, piuttosto che di risolvere specifici problemi scientifici come i numeri primi o il folding di proteine.

- Generazione blocco: 150 secondi
- Moneta totale: Nessun limite
- Algoritmo di consenso: Proof-of-work con sussidio di BOINC grid-computing
- Capitalizzazione di mercato: $122,000 millioni a metà del 2014

Alt Coins Focalizzati sull'Anonimità: CryptoNote, Bytecoin, Monero, Zerocash/Zerocoin, Darkcoin

Bitcoin e' spesso erroneamente denotata come moneta "anonima". Infatti, e' relativamente semplice connettere identita ad indirizzi bitcoin e, usando analisi dei big data, connettere gli indirizzi tra loro a formare un'immagine complessiva delle abitudini di spesa di qualcuno. Diverse alt coin mirano ad affrontare questo problema, focalizzandosi direttamente su un forte anonimato. Il primo tentativo del genere e' molto probabilmente *Zerocoin*, un protocollo a meta-moneta per preservare l'anonimato su bitcoin, introdotto con un paper al simposio IEEE del 2013 sulla Sicurezza e Privacy. Zerocoin sara implementato come una completamente separata alt coin chimata Zerocash, in sviluppo al momento della scrittura. Un approccio alternativo all'anonimato venne lanciato con *CryptoNote* in un paper pubblicato nell'ottobre del 2013. CryptoNote e' una tecnologia fondamentale che e' implementata da un certo numero di alt coin fork discussi successivamente. In aggiunta a Zerocash e CryptoNotes, ci sono diverse altre indipendenti monete anonime, come Darkcoin, che usa indirizzi stealth o transaction re-mixing per mantenere l'anonimato.

Zerocoin/Zerocash

Zerocoin è l'approccio teoretico all'anonimità della moneta digitale introdotta nel 2013 da ricercatori della Johns Hopkins. Zerocash è un'implementazione alt-coin di Zerocoin che è in via di sviluppo e non ancora rilasciata.

CryptoNote

CryptoNote e' un'implementazione di riferimento alt coin che fornisce le basi per contante digitale anonimo. Venne introdotta nell'Ottobre del 2013. E' progettata per essere forkata in diverse implementationi e ha un meccanismo di reset periodico integrato che la rende inutilizzabile come moneta stessa. Diverse alt coin sono state prodotte da CryptoNote, inclusa Bytecoin (BCN), Aeon (AEON), Boolberry (BBR), duckNote (DUCK), Fantamcoin (FCN), Monero (XMR), MonetaVerde (MCN), e Quazarcoin (QCN). CryptoNote e' inoltre nota per essere una completa implementazione ground-up di una cryptovaluta, non un fork di bitcoin.

Bytecoin

Bytecoin fu la prima implementazione prodotta da CryptoNote, offrendo una moneta anonima autosufficiente, basata su tecnologia CryptoNote. Bytecoin venne lanciata nel Luglio 2012. Notare che c'era una precedente alt coin chiamata Bytecoin con simbolo della valuta BTE, mentre la Bytecoin derivata da CryptoNote ha come simbolo della valuta, BCN. Bytecoin usa l'algoritmo proof-of-work Cryptonight, che richiede accesso ad almeno 2 MB di RAM per istanza, rendendola inadatta per GPU e ASIC mining. Bytecoin eredita ring signatures, unlinkable transactions, e anonimita della blockchain resistente all'analisi da CryptoNote.

- Generazione blocco: 2 minuti
- Totale valuta: 184 miliardi di BCN
- Algoritmo di Consenso: Cryptonight proof of work
- Capitalizzazione di mercato: $3 millioni a metà del 2014

Monero

Monero e' un'altra implementazione di CryptoNote. Ha una curva di emissione leggermente piu piatta rispetto a Bytecoin, emettendo l'80% della valuta nei primi quattro anni. Offre la stessa caratteristiche di anonimato ereditate da CryptoNote.

- Generazione blocco: 1 minuto
- Valuta totale: 18.4 million XMR
- Algoritmo di Consenso: Cryptonight proof of work
- Capitalizzazione di mercato: $5 millioni a metà del 2014

Darkcoin

Darkcoin è stato lanciato nel 2014. Darkcoin implementa un sistema di moneta anonima usando un protocollo di re-mixing (rimescolamento) per tutte le transazioni chiamato DarkSend. Darkcoin è inoltre noto per l'uso di 11 round di funzioni hash diverse (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo) per l'algoritmo di proof-of-work.

- Generazione blocco: 2.5 minuti
- Valuta totale: 22 milioni di DRK
- Algoritmo del Consenso: Multi-algoritmo a round multiplo proof of work Capitalizzazione di mercato: 19 milioni di dollari nella meta' del 2014

Alt Chain Non-Monetarie

Alt chain sono implementazioni alternative di modelli di blockchain design, che non sono usati principalmente come valuta. Molti includono una valuta, ma la valuta viene emessa come token per allocare dell'altro, come una risorsa o un contratto. La valuta, in altre parole, non e' il punto principale della piattaforma; e' una caratteristica secondaria.

Namecoin

Namecoin fu il primo fork del codice bitcoin. Namecoin e' una piattaforma decentralizzata per la registrazione ed il trasferimento di un key-value avvalendosi di una blockchain. Supporta un registro di nomi di dominio simile al sistema di nomi di dominio su internet. Namecoin e' attualmente utilizzato come un un sistema dei nomi di dominio alternativo per il dominio primario .bit. Namecoin, inoltre puo essere usato per registrare nomi e coppie di key-value in altri namespace; per memorizzare cose come indirizzi email, chiavi crittografiche, certificati SSL, firme dei file, sistemi di voto, certificati azionari: ed una miriade di altre applicazioni.

Il sistema Namecoin include la moneta Namecoin (simbolo NMC), che e' utilizzata per pagare le commissini di transazione per la registrazione ed il traferimento dei nomi. Al prezzo attuale, la commissione per registrare un nome e' 0.01 NMC o approssimativamente 1 centesimo di dollaro. Come in bitcoin, le commissioni sono trattenute dai minatori di namecoin.

I parametri base di Namecoin sono gli stessi di bitcoin:

- Tempo di generazione blocco: 10 minuti
- Valuta totale: 21 milioni di NMC nel 2140
- Algoritmo di consenso: proof of work SHA256
- Capitalizzazione di mercato: $10 milioni a metà del 2014

I namespace di Namecoin non sono limitati, e chiunque può usare qualsiasi namespace in qualunque modo. Tuttavia, alcuni namespace hanno specifiche concordate tali che quando si legge dalla blockchain, il software di livello applicativo sa come leggere e procedere da li. Se e' malformato, allora qualsiasi software si usi per leggere dallo specifico namespace mostrerà un errore. Alcuni dei namespace popolari sono:

- d/ è il namespace dei nomi dominio per i domini .bit
- id/ è il namespace per salvare gli identificatori riguardanti la persona come il suo indirizzo email, le sue chiavi PGP e così via
- u/ è una specifica addizionale più strutturata per salvare identità (basate su iopenspecs)

Il client Namecoin è molto simile a Bitcoin Core, dato che è derivato dallo stesso codice sorgente.

Dopo l'installazione, il client scaricherà una copia completa della blockchain di Namecoin e successivamente (post-sincronizzazione) sarà pronto a fare query (whois) e registrare nomi dominio. Namecoin offre tre comandi (funzioni) principali

name_new

Controlla o pre-registra un nome

name_firstupdate

Registra un nome e rendi la registrazione pubblica

name_update

Cambia i dettagli o esegui il refresh di una registrazione

Per esempio, per registrare il dominio mastering-bitcoin.bit, usiamo il comando name_new come segue:

```
$ namecoind name_new d/mastering-bitcoin
```

```
[
    "21cbab5b1241c6d1a6ad70a2416b3124eb883ac38e423e5ff591d1968eb6664a",
    "a05555e0fc56c023"
]
```

Il comando name_new registra una richiesta sul nome, creando un hash del nome con una chiave casuale. Le due stringhe ritornate da name_new sono gli hash e la chiave casuale (a05555e0fc56c023 nel precedente esempio) che puo essere usato per rendere la registrazione del nome pubblica. Una volta che la richiesta e' stata registrata sulla blockchain di Namecoin, puo essere convertita in una registrazione pubblica con il comando name_firstupdate, fornendo la chiave casuale:

```
$ namecoind name_firstupdate d/mastering-bitcoin a05555e0fc56c023 "{"map": {"www":
{"ip":"1.2.3.4"}}}}"
b7a2e59c0a26e5e2664948946ebeca1260985c2f616ba579e6bc7f35ec234b01
```

Questo esempio mapperà il nome di dominio www.mastering-bitcoin.bit all'indirizzo IP 1.2.3.4.

```
$ namecoind name_list
```

```
[
    {
        "name" : "d/mastering-bitcoin",
        "value" : "{map: {www: {ip:1.2.3.4}}}}",
        "address" : "NCccBXrRUahAGrisBA1BLPWQfSrups8Geh",
        "expires_in" : 35929
    }
]
```

Le registrazioni Namecoin necessitano di essere aggiornate ogni 36,000 blocchi (approssimativamente dai 200 ai 250 giorni). Il comando name_update non prevede alcuna commissione e quindi rinnovare i domini in Namecoin e' gratuito. Fornitori terzi possono gestire la registrazione, il rinnovo automatico, ed aggiornare via interfaccia web, per una piccola commissione. Con un fornitore terzo si evita il bisogno di lanciare un client Namecoin, ma si perde il controllo indipendente di un registro di nomi decentralizzato offerto da Namecoin.

Ethereum

Ethereum e' una piattaforma per il processo e l'esecuzione di contratti Turing-completi basato su un libro contabile blockchain. Non e' un clone di Bitcoin, ma una implementazione e design completamente indipendente. Ethereum ha una moneta integrata, chiamata *ether*, che e' richiesta per pagare l'esecuzione di un contratto. La blockchain di Ethereum registra *contratti*, che sono espressi in un linguaggio Turing-completo di basso livello, byte code-like. Essenzialmente, un contratto e' un programma che gira su ogni nodo nel sistema Ethereum. I contratti Ethereum possono memorizzare dati, inviare e ricevere pagamenti di ether, memorizzare ether, ed eseguire una gamma infinita (da cui Turing-completo) di azioni calcolabili, agendo come agenti decentralizzati di sofware autonomo.

Ethereum puo implementare sistemi abbastanza complessi che sono altrimenti implementati come alt chain stesse. Ad esempio, il seguente e' un contratto di registrazione di nomi Namecoin-like scritto in Ethereum (o piu precisamente, scritto in un linguaggio di alto livello che puo essere compilato per codice Ethereum):

```
if !contract.storage[msg.data[0]]: # La chiave è ancora disponibile?
    # Allora prendila!
    contract.storage[msg.data[0]] = msg.data[1]
    return(1)
else:

    return(0) // Altrimenti non fare niente
```

Il Futuro delle Valute

Il futoro delle monete crittografiche complessivamente e' anche piu lucente rispetto al futuro di bitcoin. Bitcoin introdusse un forma completamente nuova di organizzazione decentralizzata e di

consenso che ha prodotto centinaia di innovazioni incredibili. Queste invenzioni probabilmente interesseranno ampi settori dell'economia, dalla scienza dei sistemi distribuiti alla finanza, economia, valute, il sistema bancario centrale, e la gestione aziendale. Molte attività umane che precedentemente richiedevano istituzioni o organizzazioni centralizzate per funzionare come punti di controllo autorevoli o di fiducia, possono ora essere decentralizzate. L'invenzione di blockchain e del sistema di consenso ridurrà significativamente il costo di organizzazione e coordinamento su sistemi a larga scala, riducendo al contempo le occasioni di concentrazione di potere, corruzione e cattura della regolamentazione (ndt parti di stato che favoriscono aziende).